IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application. No.	: 10/045,893	Confirmation No.	: 3131
1st Named Inventor	: Adusumilli	Art Unit	: 2134
Filed	: 01/12/2002	Examiner	: Brown, Christopher J.
Docket No.	: 42390.P12318X	Customer No.	: 7590

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

This brief is in furtherance of the Notice of Appeal, filed in the above-captioned case on November 07, 2008. Applicants (hereafter "Appellants") hereby submit this Brief (37 C.F.R. § 41.37). The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying Transmittal of Appeal Brief. Appellants respectfully request consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37c(1)):

Page 18 of this brief bears the practitioner's signature.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California, 95052, to whom the invention is assigned.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

With respect to other appeals or interferences that may affect, or may be affected by, or may have a bearing on the Board's decision in this appeal, to the best of Appellant's knowledge, there is only one other possible such appeal. In particular, there is an appeal underway in U.S. Patent Application Serial No. 10/000,154, which is a parent to the present patent application.

III. STATUS OF THE CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

The status of the claims in this application are:

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims 33-60 are currently pending in the application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 1-32
2. Claims withdrawn from consideration but not cancelled: NONE
3. Claims pending: 33-60
4. Claims allowed: NONE
5. Claims rejected: 33-60

C. CLAIMS ON APPEAL

Claims 33-60 are on appeal.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

A response was submitted on 5/21/08 in response to the Non-Final Office Action mailed on 2/22/08. The response includes amendments to the claims. As understood by Appellant, the Examiner has entered the amendments. A copy of all claims on appeal is attached hereto as an appendix of claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

Independent claim 33 pertains to an apparatus (e.g., security system 160 in FIG. 1; security system 345 in FIG. 3; security system 1312 in FIGs. 13, 14, 15, and 19; security system 2300 in FIG. 23), according to a first embodiment of the invention. The apparatus is to reside in a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19) coupled between a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) of the data center. The apparatus comprises a first interface (e.g., network interface 350 in FIG. 3, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to the public network to receive Secure Sockets Layer (SSL) encrypted data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4) from at least one wired client device (e.g., wired access device 320 in FIG. 3) and to receive Wireless Transport Layer Security (WTLS) encrypted data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) from at least one wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises client-type determining logic (e.g., selection system 360 in FIG. 3, selection system 800 in FIG. 8) to determine whether a client device requesting a secure connection is a wired client device (e.g., wired access device 320 in FIG. 3) or a wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises logic to perform a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) to establish the secure connection when it is determined that the requesting client device is the wired client device (e.g., wired access device 320 in FIG. 3). The apparatus also comprises logic to perform a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) to establish the secure connection when it is determined that the requesting client device is the wireless client device (e.g., wireless access device 305 in FIG. 3). The apparatus also comprises logic to

convert the SSL encrypted data to an unencrypted format (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23) and to convert the WTLS encrypted data to an unencrypted format (e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23). The apparatus also comprises a second interface (e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the data in the unencrypted formats to the server of the data center.

Independent claim 42 pertains to a method (see e.g., FIG. 4, FIG. 12, etc.), according to a first embodiment of the invention. The method comprises receiving data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4) (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) within a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19) through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) from at least one wired client device (e.g., wired access device 320 in FIG. 3) and at least one wireless client device (e.g., wireless access device 305 in FIG. 3) each requesting a secure connection with a server of the data center (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19). The method also comprises performing a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) to establish the secure connection with the wired client device. The method also comprises performing a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) to establish the secure connection with the wireless client device. The method also comprises converting the data from an encrypted format to an unencrypted format (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23; and e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23). The method also comprises providing the data in the unencrypted format to the server of the data center through an interface (e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19).

Independent claim 50 pertains to an article comprising a machine-readable medium having stored thereon instructions that if executed cause a machine to perform operations (e.g., paragraph [0039]-[0040] and original claim 26), according to a first embodiment of the invention. The operations comprise receiving first encrypted data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4) through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) from at least one wired client device (e.g., wired access device 320 in FIG. 3) and second encrypted data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) through the public network from at least one wireless client device (e.g., wireless access device 305 in FIG. 3) each requesting a secure connection with a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) within a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19). The operations also comprise performing a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) to establish the secure connection with the wired client device. The operations also comprise performing a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) to establish the secure connection with the wireless client device. The operations also comprise converting the first encrypted data to a plain data format and converting the second encrypted data to a plain data format (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23; and e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23). The operations also comprise providing the converted data in the plain data formats to the server through an interface (e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19). The machine-readable medium comprises one of a disk and a memory (paragraph [0039]-[0040]).

Independent claim 56 pertains to an apparatus (e.g., security system 160 in FIG. 1; security system 345 in FIG. 3; security system 1312 in FIGs. 13, 14, 15, and 19; security system

2300 in FIG. 23), according to a first embodiment of the invention. The apparatus comprises a network interface (e.g., network interface 350 in FIG. 3, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to receive Secure Sockets Layer (SSL) data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4) from a wired device through a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and Wireless Transport Layer Security (WTLS) data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) from a wireless device through a public network. The apparatus also comprises Public Key Infrastructure (PKI) logic (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) to establish a secure connection with the wired device. The apparatus also comprises Wireless Public Key Infrastructure (WPKI) logic (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) to establish a secure connection with the wireless device. The apparatus also comprises SSL logic (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23) to convert the SSL data to another format. The apparatus also comprises WTLS logic (e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23) to convert the WTLS data to another format. The apparatus also comprises a second interface (e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the data converted from the SSL and WTLS formats to a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) over a private network.

Independent claim 59 pertains to a single network device (e.g., security system 160 in FIG. 1; security system 345 in FIG. 3; security system 1312 in FIGs. 13, 14, 15, and 19; security system 2300 in FIG. 23), according to a first embodiment of the invention. The single network device is to be coupled within a data center (e.g., data center 150 in FIG. 1; data center 340 in FIG. 3; data center 1316 in FIGs. 13, 14, 15, and 19) between a public network (e.g., public network 120 in FIG. 1, public network 325 in FIG. 3, public network 1310 in FIGs. 13, 14, 15, and 19) and a server (e.g., server 390 in FIG. 3; server 1314 in FIGs. 13, 14, 15, and 19) of the

data center. The single network device comprises a first interface (e.g., network interface 350 in FIG. 3, interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to the public network, the first interface to receive first data (e.g., SSL data received on port 352 in FIG. 3; block 455 in FIG. 4) that has been encrypted according to a wired encryption protocol from a wired device, and the first interface to receive second data (e.g., WTLS data received on port 354 in FIG. 3, block 430 in FIG. 4) that has been encrypted according to a wireless encryption protocol from a wireless device. The single network device also comprises logic to perform a wired authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case SSL in FIG. 12, block 1806 in FIG. 18, PKI module 2308 in FIG. 23) with the wired device. The single network device also comprises logic to perform a wireless authentication (e.g., blocks 1106 and 1108 in FIG. 11; complete authentication for case WTLS in FIG. 12, block 1706 in FIG. 17, WPKI module 2310 in FIG. 23) with the wireless device. The single network device also comprises logic to convert the first data to first unencrypted data (e.g., SSL conversion system 374 in FIG. 3, SSL module 2304 in FIG. 23) and to convert the second data to second unencrypted data (e.g., WTLS conversion system 372 in FIG. 3, WTLS module 2306 in FIG. 23). The single network device also comprises a second interface (e.g., network interface 380 in FIG. 3; interface inherent for security system 1312 in FIGs. 13, 14, 15, and 19) to provide the first and second unencrypted data to the server of the data center.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

A. Claims 33-36, 38, 40, 42, 43, 45, 48, 50-52, and 54-59 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,571,221 to Stewart in view of U.S. Pub. No. 2002/0099957 by Kramer in view of U.S. Patent No. 7,099,284 to Halme.

ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

A. REJECTION OF CLAIMS 33-36, 38, 40, 42, 43, 45, 48, 50-52, AND 54-59 UNDER 35 U.S.C. § 103(A) AS BEING UNPATENTABLE OVER U.S. PATENT NO. 6,571,221 TO STEWART (HEREINAFTER "STEWART") IN VIEW OF U.S. PUB. NO. 2002/0099957 BY KRAMER (HEREINAFTER "KRAMER") IN VIEW OF U.S. PATENT NO. 7,099,284 TO HALME (HEREINAFTER "HALME") IS BELIEVED TO BE IMPROPER

GROUP I: CLAIMS 33-55, 59, and 60

Appellants respectfully submit that the claims of Group I are allowable over Stewart, Kramer, and Halme.

Claim 33 pertains to:

"*An apparatus **to reside in a data center coupled between a public network and a server of the data center**, the apparatus comprising:*

***a first interface to the public network** to receive **Secure Sockets Layer (SSL)** encrypted data from at least one wired client device and to receive **Wireless Transport Layer Security (WTLS)** encrypted data from at least one wireless client device;*

client-type determining logic to determine whether a client device requesting a secure connection is a wired client device or a wireless client device;

logic to perform a wired authentication to establish the secure connection when it is determined that the requesting client device is the wired client device;

logic to perform a wireless authentication to establish the secure connection when it is determined that the requesting client device is the wireless client device;

***logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data to an unencrypted format;** and*

***a second interface to provide the data in the unencrypted formats to the server of the data center**".*

Stewart, Kramer and Halme do not disclose these limitations or render them obvious.

Stewart pertains to a network communication service with an improved subscriber model using digital certificates. See e.g., the Title. However, Stewart does not disclose or render

obvious the claimed apparatus **to reside in a data center coupled between a public network and a server of the data center** that comprises **a first interface to the public network** to receive **SSL** and **WTLS** encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Firstly, as understood by Applicants, Stewart does not disclose logic to convert the SSL and WTLS encrypted data to unencrypted formats. In fact, Stewart does not even appear to mention "WTLS". The Examiner appears to agree, since on page 3 of the present Office Action, the Examiner has stated that "*Stewart does not teach SSL, WTLS or converting encrypted data to an unencrypted format*".

Secondly, in rejecting claim 33, the Examiner has relied upon features of both the hybrid wired and wireless access point 124 and the service provider 140. See e.g., page 4 of the present Final Office Action. For example, on page 4 of the present Final Office Action, the Examiner references column 8, lines 47-55 which describes hybrid wired and wireless access point 124, and column 14, lines 29-44 which describes actions by network or service provider 140. However, Applicants respectfully submit that it is inappropriate. The hybrid wired and wireless access point 124 and the service provider 140 are different components and are separated by a centralized network 130. Column 8, line 65 indicates that network 130 is preferably the Internet. Different components 124, 140 separated by network 130, preferably the Internet, do not meet the limitations of claim 33. Claim 33 recites that the apparatus is to reside in a data center coupled between a public network and a server of the data center and has the claimed first interface to the public network and the claimed second interface to provide the data in the unencrypted formats to the server of the data center. The hybrid wired and wireless access point 124 does not reside in a data center coupled between a public network and a server of the data

center and does not have a second interface to provide the data in the unencrypted formats to the server of the data center.

Thirdly, Stewart does not disclose or render obvious an apparatus that is to reside in a data center coupled between a public network and a server of the data center and has the claimed first interface to the public network and the claimed second interface to provide the data in the unencrypted formats to the server of the data center. As discussed above, the hybrid wired and wireless access point 124 does not reside in a data center coupled between a public network and a server of the data center and does not have a second interface to provide the data in the unencrypted formats to the server of the data center. Moreover, Stewart does not disclose that the service provider 140 have a second interface to provide data in the unencrypted formats to a server of a data center.

Kramer does not remedy all of what is missing from Stewart. Kramer discusses establishing a secure connection with a private corporate network over a public network. See e.g., the Title. Kramer discusses in paragraph [0050] "*the external client secures the connection 430*" and that "*The security for the connection may be provided by using Secured Socket Layer (SSL) protocol or Wireless Transport Layer Security (WTLS) security*". However, as understood by Applicants, the SSL and the WTLS are used by the "*external client*" (e.g., external client 340). The external client 340 does not reside in a data center coupled between a public network and a server of the data center. Furthermore, Kramer does not disclose that the VPN access server 314 has logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data to an unencrypted format. Kramer does not even disclose that the VPN access server 314 receive WTLS data. It should not be assumed that just because the external client uses WTLS that the VPN access server 314 would receive WLTS. Rather, as understood by Applicants, conversion from WTLS to another format (e.g., SSL) would typically be performed before reaching the VPN access server 314 e.g., in a WAP gateway of the like.

In the response to arguments section on the top half of page 3 of the present Final Office Action, the Examiner appears to have argued that it is appropriate to interpret that the VPN access server 314 may receive WTLS data. One reason the Examiner has given is that the external device and the access server use the same protocol, since a connection requires two parties. However, this simply ignores the conversion from WTLS to another format (e.g., SSL) that would typically be performed e.g., in a WAP gateway or the like. For example a cell phone may use WTLS but a server in communication with the cell phone would typically not receive WTLS but rather SSL or some other wired format after the WTLS data was converted, for example, in a WAP gateway. Another reason that the Examiner has given is that Kramer does not teach a conversion prior to the VPN access server. Appellants note that Kramer has a very limited discussion of SSL and WTLS. The fact that Kramer does not elaborate on SSL and WTLS, would seem to indicat that Kramer intends the SSL and WTLS to operate conventionally, which as understood by Appellants would mean that WTLS data would not be passed all the way from external client 340 to VPN access server 314. Moreover, Kramer does not disclose that VPN access server 314 has a wireless transceiver to receive WTLS encrypted data.

Accordingly, Kramer does not appear to disclose **an apparatus to reside in a data center coupled between a public network and a server of the data center** that includes a first interface to the public network to receive SSL data and to receive **WTLS data**. Additionally, Kramer does not appear to disclose **an apparatus to reside in a data center coupled between a public network and a server of the data center** that includes logic to convert the SSL encrypted data to an unencrypted format and to **convert the WTLS encrypted data to an unencrypted format**. As discussed above, Stewart also does not disclose such an apparatus.

Halme does not remedy all of what is missing from Stewart and Kramer. Halme discusses a data transmission control and performance monitoring method of an IPSEC link in a virtual private network. See e.g., the Title. However, Halme does not disclose or render obvious an apparatus **to reside in a data center coupled between a public network and a server of the**

data center that comprises **a first interface to the public network** to receive SSL and WTLS encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Accordingly, Stewart, Kramer and Halme do not disclose or render obvious the claimed apparatus **to reside in a data center coupled between a public network and a server of the data center** that comprises **a first interface to the public network** to receive SSL and WTLS encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Accordingly, even if combined, the references do not disclose all limitations.

Moreover, there is no suggestion or motivation to make the Examiner's proposed combination. Furthermore, the Examiner has not articulated with enough detail what the exact combination would be, or why it would be obvious to make this particular combination. It would seem that modifications to the references not taught in the art would likely be necessary in order to modify the references in the manner proposed by the Examiner.

Appellants respectfully submit that it is inappropriate to use the claim as an instruction manual or template to piece together the teachings of the prior art so that the claim is rejected as being. Appellants respectfully submit that it is inappropriate to use hindsight reconstruction to pick and choose among seemingly isolated disclosures in the prior art to deprecate the claim.

For at least one or more of these reasons, claim 33, and its dependent claims, are believed to be allowable over Stewart, Kramer and Halme.

Independent claims 42 and 50, and their respective dependent claims, are believed to be allowable for one or more similar reasons.

GROUP II: CLAIMS 56-58

Appellants respectfully submit that the claims of Group II are allowable over Stewart, Kramer, and Halme.

Claim 56 pertains to:

"*An apparatus comprising:*

a network interface** to receive **Secure Sockets Layer (SSL) data** from a wired device through a public network and **Wireless Transport Layer Security (WTLS) data** from a wireless device **through a public network;

***Public Key Infrastructure (PKI) logic** to establish a secure connection with the wired device;*

***Wireless Public Key Infrastructure (WPKI) logic** to establish a secure connection with the wireless device;*

***SSL logic** to convert the SSL data to another format;*

***WTLS logic** to convert the WTLS data to another format; and*

a second interface to provide the data converted from the SSL and WTLS formats to a server over a private network".

Stewart, Kramer and Halme do not disclose these limitations or render them obvious. In particular, Stewart, Kramer and Halme do not disclose or render obvious an apparatus that has **a network interface to receive SSL data and WTLS data through a public network, and that has a second interface to provide data converted from the SSL and WTLS formats to a server over a private network.** The discussion above is pertinent to this point.

In addition, Stewart, Kramer and Halme do not disclose or render obvious an apparatus that has a network interface to receive SSL data and WTLS data through a public network, and that has a second interface to provide data converted from the SSL and WTLS formats to a server over a private network, and that also has **Public Key Infrastructure (PKI) logic and Wireless Public Key Infrastructure (WPKI) logic.** In particular, neither Stewart, Kramer, or

Halme, appear to even mention a Wireless Public Key Infrastructure (WPKI) logic, let alone the particular claimed WPKI logic in the particular claimed apparatus.

Accordingly, even if combined, the references do not disclose all limitations.

Moreover, there is no suggestion or motivation to make the Examiner's proposed combination. Furthermore, the Examiner has not articulated with enough detail what the exact combination would be, or why it would be obvious to make this particular combination. It would seem that modifications to the references not taught in the art would likely be necessary in order to modify the references in the manner proposed by the Examiner.

Appellants respectfully submit that it is inappropriate to use the claim as an instruction manual or template to piece together the teachings of the prior art so that the claim is rejected as being. Appellants respectfully submit that it is inappropriate to use hindsight reconstruction to pick and choose among seemingly isolated disclosures in the prior art to deprecate the claim.

For at least one or more of these reasons, claim 56 and its dependent claims are believed to be allowable over Stewart, Kramer and Halme.

CONCLUSION

Based on the foregoing, Appellants request that the Board overturn the rejection of all pending claims and hold that all of the claims of the present application are allowable.

Appellants respectfully petition for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17 for such an extension.

Please charge any shortages and credit any overpayment to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 12/31/08

By Brent E. Vecchia

Brent E. Vecchia, Reg. No. 48,011
Tel.: (303) 740-1980 (Mountain Time)

1279 Oakmead Parkway
Sunnyvale, California 94085-4040

VII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal are:

1-32. (Cancelled)

33. (Previously Presented) An apparatus to reside in a data center coupled between a public network and a server of the data center, the apparatus comprising:

a first interface to the public network to receive Secure Sockets Layer (SSL) encrypted data from at least one wired client device and to receive Wireless Transport Layer Security (WTLS) encrypted data from at least one wireless client device;

client-type determining logic to determine whether a client device requesting a secure connection is a wired client device or a wireless client device;

logic to perform a wired authentication to establish the secure connection when it is determined that the requesting client device is the wired client device;

logic to perform a wireless authentication to establish the secure connection when it is determined that the requesting client device is the wireless client device;

logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data to an unencrypted format; and

a second interface to provide the data in the unencrypted formats to the server of the data center.

34. (Previously Presented) The apparatus of claim 33, wherein the second interface is to receive data in an unencrypted format from the server.

35. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication comprises logic to perform the authentication using a wired communication protocol, and wherein the logic to perform the wireless authentication comprises logic to perform the authentication using a wireless communication protocol.

36. (Previously Presented) The apparatus of claim 35, wherein the logic to perform the wired authentication comprises logic to perform the authentication using a Public Key Infrastructure (PKI) protocol and wherein the logic to perform the wireless authentication comprises logic to perform the authentication using a Wireless Public Key Infrastructure (WPKI) protocol.

37. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to determine if the requesting client device has requested authentication of the server; and

logic to transmit a server digital certificate for the server when it is determined that the requesting client device has requested the authentication of the server.

38. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to generate a request for a digital certificate from the requesting client device; and

logic to authenticate a digital certificate received from the requesting client device.

39. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to retrieve a client digital certificate using a Uniform Resource Locator received from the requesting client device; and

logic to authenticate a retrieved client digital certificate.

40. (Previously Presented) The apparatus of claim 33, wherein the client-type determining logic comprises:

logic to determine a security protocol used for an encrypted request from the requesting client device; and

logic to determine whether the requesting client device is the wired client device or the wireless client device dependent on the determined security protocol.

41. (Previously Presented) The apparatus of claim 33, further comprising:

logic to receive a client digital signature; and

logic to validate the received client digital signature.

42. (Previously Presented) A method comprising:

receiving data within a data center through a public network from at least one wired client device and at least one wireless client device each requesting a secure connection with a server of the data center;

performing a wired authentication to establish the secure connection with the wired client device; and

performing a wireless authentication to establish the secure connection with the wireless client device;

converting the data from an encrypted format to an unencrypted format; and

providing the data in the unencrypted format to the server of the data center through an interface.

43. (Previously Presented) The method of claim 42, wherein said performing the wired authentication comprises performing the authentication using a wired communication protocol and wherein said performing the wireless authentication comprises performing the authentication using a wireless communication protocol.

44. (Previously Presented) The method of claim 42, wherein said performing the wired authentication and said performing the wireless authentication each comprises:

determining if the requesting client device has requested authentication of the server; and

transmitting a server digital certificate for the server when it is determined that the requesting client device has requested the authentication of the server.

45. (Previously Presented) The method of claim 42, wherein each of said performing the wired authentication and said performing the wireless authentication comprises:

generating a request for a digital certificate from the requesting client device; and

authenticating a digital certificate received from the requesting client device.

46. (Previously Presented) The method of claim 45, wherein said authenticating the digital certificate includes verifying a validity period of the client digital certificate.

47. (Previously Presented) The method of claim 42, wherein each of said performing the wired authentication and said performing the wireless authentication comprises:

retrieving a client digital certificate using a Uniform Resource Locator received from the requesting client device; and

authenticating the retrieved client digital certificate.

48. (Previously Presented) The method of claim 42, further comprising:

determining a security protocol used for an encrypted request; and

determining whether the requesting client device is a wired client device or a wireless client device dependent on the determined security protocol.

49. (Previously Presented) The method of claim 42, further comprising:

receiving a client digital signature; and

validating the received client digital signature.

50. (Previously Presented) An article comprising a machine-readable medium having stored thereon instructions that if executed cause a machine to perform operations comprising:

receiving first encrypted data through a public network from at least one wired client device and second encrypted data through the public network from at least one wireless client device each requesting a secure connection with a server within a data center;

performing a wired authentication to establish the secure connection with the wired client device; and

performing a wireless authentication to establish the secure connection with the wireless client device; and

converting the first encrypted data to a plain data format and converting the second encrypted data to a plain data format; and

providing the converted data in the plain data formats to the server through an interface,

wherein the machine-readable medium comprises one of a disk and a memory.

51. (Previously Presented) The article of claim 50, wherein the instructions to perform the wired authentication further comprise instructions that if executed cause the machine to perform operations comprising authentication using Public Key Infrastructure (PKI) protocol, and wherein the instructions to perform the wireless authentication further comprise instructions that if executed cause the machine to perform operations comprising authenticating using Wireless Public Key Infrastructure (WPKI) protocol.

52. (Previously Presented) The article of claim 50, wherein the instructions to perform each of the wired authentication and the wireless authentication comprise instructions that if executed cause the machine to perform operations comprising:

generating a request for a digital certificate from the requesting client device; and

authenticating a digital certificate received from the requesting client device.

53. (Previously Presented) The method of claim 42, further comprising updating a short-lived server certificate from a certificate authority repository based on a user defined interval.

54. (Previously Presented) The method of claim 42, wherein said performing the wired authentication comprises performing the wired authentication based on Public Key

Infrastructure (PKI), and wherein said performing the wireless authentication comprises performing the wireless authentication based on Wireless Public Key Infrastructure (WPKI).

55. (Previously Presented) The method of claim 42, further comprising:

performing a security format conversion for encrypted data received from the wired device; and

performing a security format conversion for encrypted data received from the wireless device.

56. (Previously Presented) An apparatus comprising:

a network interface to receive Secure Sockets Layer (SSL) data from a wired device through a public network and Wireless Transport Layer Security (WTLS) data from a wireless device through a public network;

Public Key Infrastructure (PKI) logic to establish a secure connection with the wired device;

Wireless Public Key Infrastructure (WPKI) logic to establish a secure connection with the wireless device;

SSL logic to convert the SSL data to another format;

WTLS logic to convert the WTLS data to another format; and

a second interface to provide the data converted from the SSL and WTLS formats to a server over a private network.

57. (Previously Presented) The apparatus of claim 56, wherein the apparatus is to reside in a data center between the public network and the data center server.

58. (Previously Presented) The apparatus of claim 56, wherein the other format is a plain data format, and wherein the PKI logic, the WPKI logic, the SSL logic, and the WTLS logic are all included within a single device.

59. (Previously Presented) A single network device to be coupled within a data center between a public network and a server of the data center, the single network device comprising:

a first interface to the public network, the first interface to receive first data that has been encrypted according to a wired encryption protocol from a wired device, and the first interface to receive second data that has been encrypted according to a wireless encryption protocol from a wireless device;

logic to perform a wired authentication with the wired device;

logic to perform a wireless authentication with the wireless device; and

logic to convert the first data to first unencrypted data and to convert the second data to second unencrypted data; and

a second interface to provide the first and second unencrypted data to the server of the data center.

60. (Previously Presented) The apparatus of claim 33,

wherein the logic to perform the wired authentication comprises logic to verify a certificate from the wired client device, logic to check a certificate revocation list, and logic to provide a server side certificate;

wherein the logic to perform the wireless authentication comprises logic to verify a certificate from the wireless client device and logic to provide a server side certificate.

VIII. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

To the best of Appellant's knowledge, no evidence has been submitted pursuant to 37 CFR Sections 1.130, 1.131, or 1.131.

IX. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

To the best of Appellant's knowledge, no decisions have been rendered by the board in the appeal underway in U.S. Patent Application Serial No. 10/000,154, which is a parent to the present patent application. Appellants believe that any such decisions when they become available will be readily available to the board, alternatively, Applicants will provide any decisions specifically requested.